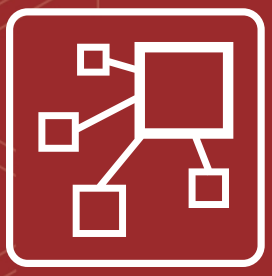


FORTINET
High Performance Network Security

FortiGate Connector for Cisco ACI Device Package - Release Notes

Version 2.0

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FORTINET PRIVACY POLICY

https://www.fortinet.com/corporate/about-us/privacy.html

FEEDBACK

Email: techdocs@fortinet.com

Thursday, January 25, 2018

FortiGate Connector for Cisco ACI Device Package v2.0 - Release Notes

01-563-371310-20180125

TABLE OF CONTENTS

Change Log

Date	Change Description
2018-01-12	Initial release for v.2.0

FortiGate Connector for Cisco ACI Device Package v.2.0

Introduction

This document provides the following information for FortiGate Connector for Cisco ACI Device Package v2.0..
This product can also be referred to as FortiGate Connector v2.0 for Cisco ACI v3.x.

Supported Models

FortiGate Connector for Cisco ACI Device Package v2.0 supports the following additional predefined models:

- FG-300D
- FG-600D
- FG-800D
- FG-900D
- FG-1000C
- FG-1000D
- FG-1200D
- FG-1500D
- FG-3000D
- FG-3100D
- FG-3200D
- FG-3700D
- FG-7040E
- FG-VM

Unknown models

The use of Fortigate Connector can be attempted with any Fortigate models, but do so with caution. Only those listed above have been confirmed. If an unknown model of Fortigate is used, the user needs to verify port names match the actual Fortigate model.

New Features

- Support Hybrid Mode
- Support Customized Dynamic EPG group
- Support BGP
- Support Security Zone

Special Notices

Device Package Version Compatibility

This device package is not backward compatible with release 1.3.x Device Package or beta release of 2.0.x. Any configuration that was done using Device Package 1.3.x or beta 2.0.x will not be importable into this release.

Hybrid Vs Non-Hybrid Mode

Customer can use this version via none-hybrid mode and the behavior will be the same as Device Package 1.3.x. For Hybrid mode, only the networking and Customized Dynamic EPG functions will be automated while the rest will be ignored. Ex: Network Configuration such as Device Interface, Security Zone, Static Route and BGP/OSPF will be programmed and monitor by Cisco ACI. Other components relating to Firewall configuration will be ignore and user will have to manually configure them within Fortigate itself.

Hybrid / Non-Hybrid Mode Option Field Lock

It is advice to have the Hybrid/Non-Hybrid Field locked. Toggling between Hybrid and Non-Hybrid Mode or vice versa via “Service Modification” will triggered unexpected behavior. Therefore, it is recommended to lock this field.

“VDOM Interfaces Consumer/Provider Addrgrp” Options under VDOM-Folder Lock (Dynamic EPG)

It is advice to have the “VDOM Interfaces Consumer/Provider Addrgrp” also known as Dynamic EPG Consumer/Provider under VDOM Folder locked. In case customer changed the Group mapping after Service Graph has deployed, Address Group members will appear in the new group as well as the old group. Customer will have to manually remove the members from the old Address Group.

Dynamic EPG Function

Dynamic EPG function was introduced in Device Package 1.x, and the behavior will supersede with this release moving forward.

Security Zone

Security Zone is a new feature for this release to allow adding interface members into the zone for better management in case of multigraphs with shared Vdom scenario.

BGP

BGP is also supported with this release. The implementation of this routing protocol is same as OSPF. However only iBGP is supported base on Cisco ACI's supportiveness.

Fortigate OS Compatibility

We have tested FortiOS 5.6 for this release.

Predefined keywords

Do not modify the predefined key words used by FortiGate.

Custom Addresses and Services character limitations

The name fields of Firewall Addresses and Services should not include spaces or special characters.

VDOM name limitations

Beginning with FortiGate Connector v1.2, VDOM name is no longer a configurable option due to design recommendation from Cisco. The VDOM name will be the virtual device ID. After a service graph is deployed, a virtual Device ID is randomly assigned by Cisco APIC and that will be the VDOM name appears on Fortigate. However, in the VDOM name comments field it will display the ACI Tenant information so customer can get an idea between Tenants to Vdom association.

Rule ID sequence and Policy Name

Rule ID with lowest number will get processed and listed first on the FortiGate. In addition, if deploying multiple service graphs shared with same virtual device, please ensure Rule IDs and Policy Names are unique otherwise, they will override each other.

BGP/OSPF Configuration

User doesn't need to perform any BGP/OSPF parameter configuration except Router ID configured in Router Configurations under L4-L7 services. The recommendation from Cisco is that user creates BGP/OSPF Configuration on L3OUTs which is the corresponding interface configuration along with all BGP/OSPF parameters to the FortiGate on APIC. During the Service Graph deployment, Fortigate Connector device package will extract the BGP/OSPF parameters from APIC and then program the corresponding BGP/OSPF configurations on FortiGate.

Transparent Mode and NAT Mode Configuration

Beginning with FortiGate FortiConnector v1.2, the device package no longer has the option to select VDOM mode. When Go-Through mode is selected, interface ip address field must be in default setting; when "GoTo" mode is selected, interface ip addresses must be configured with valid ip address and network mask. This restriction however lifted as of Cisco ACI v2.0(2I).

Static Route Sequence Number

For Static Route Sequence Number of 0 (default value), Device Package will ignore static route programming. Otherwise, Device Package will program any entry in the Static Route fields when Sequence Number is greater than 0.

Faults Report

When Device Package returned fault(s) to Cisco ACI due to various reasons, the fault message(s) will show up in Cisco ACI System level instead of Tenant level. However, you will still see the fault from the debug.log file.

We also observed on some occasion when we report fault code to Cisco ACI, but ACI will not show up nor will it take any action. The work around would be to remove the service graph and redeploy again.

Empty Entries under Parameter Folder

There is an issue we found when we leave Folder/Parameter fields empty when they previously have existing entries. The device package will not be able to fallback to default value which causes no update for those Parameter(s). Example: We applied a Service Graph with Customer Firewall Address Group by selecting "Show in Address List" option to be "enable". If we clear this field by clicking on the "x" box (**Figure 1**) will result in clearing all options within it (**Figure2**). By clearing this field, the default value should be "disable" but our device package will not be able to handle it. The workaround is to change the option from "enable" to "disable" instead of leaving the field empty. This behavior will affects all other Folder/Parameter until we fix it in a later release.

Figure 1 - Clearing the field

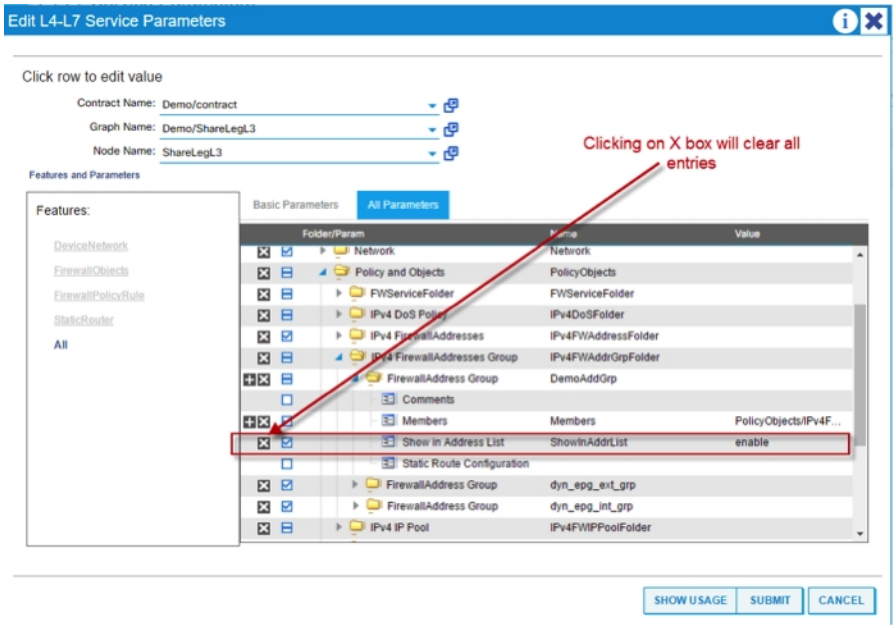
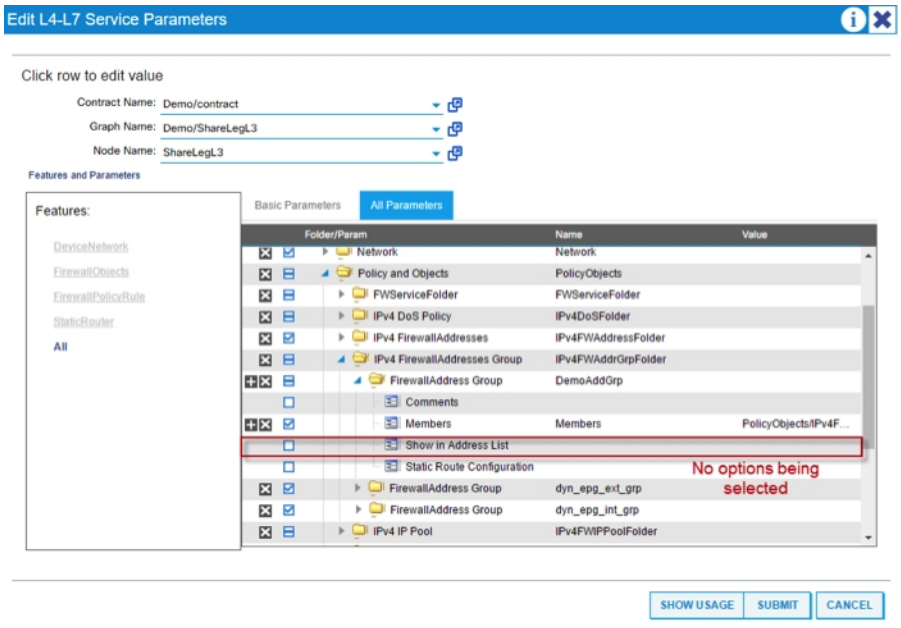


Figure 2 - Options cleared



Product Integration and Support

Fortinet Products

This Version of FortiGate Connector for Cisco ACI Device Package is compatible with the following firmware:

- FortiOS 5.6.x

Cisco Environment

This Version of FortiGate Connector for Cisco ACI Device Package is supported by the following Cisco ACI environments:

Cisco ACI v3.0(2k) or above

Known Issues

The following issues have been identified in version 2.0. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Bug ID	Description
403172	Administrative priority from static route cannot add value to 4294967295. Cisco ACI only supports up to 9 Digital entries.
380069	When Service Graph generated Fault, the Fault message will display at System Level instead of Tenant Level. Cisco has been notified on this issue.
461798	OSPF Area ID provided by Cisco is incorrect causing device package to have traceback. (The OSPF Area ID provided by Cisco is always area “1” which caused a traceback within our code.) Cisco has been notified on this issue and the work around is to use area “1” or mixed of area “x” along with area “1” in case of two arm scenario.
466791	Redistribution for “static” and “connected” are not enabled when ospf and bgp protocols are used

Known issues from previous versions not listed here have been resolved.

FORTINET

High Performance Network Security